Stand Up For Digital Rights!

Recommendations for Responsible Tech

Executive Summary

Introduction[1]

Recent years have seen the formation of private sector empires in the online world that hold unprecedented power over how people access information and communicate. Although these tech giants earned their position by developing new and innovative products, and their businesses support the spread of the Internet, the growing power of private sector intermediaries[2] over online communications has important implications. The enormous impact their policies and practices have on the exercise of key rights means that they are on the cutting edge of the application of new ideas about the human rights responsibilities of private actors.

An important starting point for any discussion about human rights and the Internet is that human rights standards apply to the online world. The Internet supports the promotion and protection of a number of human rights, most obviously freedom of expression but also the rights to association, to education, to work, to participate

[1] This publication was drafted by Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy, with editing and support from Toby Mendel, Executive Director, Centre for Law and Democracy. Supporting material was provided by the Arabic Network for Human Rights Information, the Centre for Internet and Society, the Centro de Estudios en Libertad de Expresión y Acceso a la Información, Open Net Korea, Tamir Israel and Christopher Parsons. Additional research was provided by CLD's interns and pro bono students: Pierre-Luc Bergeron, Alice Bodet-Lamarche, Jim Boyle, Ken Cadigan, Paul Calderhead, Laurent Fastrez, Claire MacLean, Jonathan Marchand, Charles McGonigal, Virginia Nelder and Leslie Whittaker. For more information about this project, please visit https://www.responsible-tech.org.

[2] We define "intermediaries" as private sector bodies whose online operations somehow, whether directly or indirectly, facilitate communication between two or more parties over the Internet.

and to take part in cultural life, among others. The UN Human Rights Council[3] and the UN General Assembly[4] have both affirmed that human rights standards apply to the online world. The Internet supports human rights by improving communications and information sharing, by providing a voice for human rights defenders, and by strengthening democratic society through its contribution to political, social, cultural and economic development. However, the role that private sector intermediaries play in providing access to, managing, facilitating and mediating online speech presents a key challenge to guaranteeing human rights on the Internet, particularly as traditionally public avenues for expression, such as the postal service, are being replaced by private services.

Although States bear the primary obligation for ensuring respect for human rights, it is now recognised that private sector actors also have a direct responsibility to respect and to foster respect for human rights. A key issue for guaranteeing freedom of expression on the Internet is the role that online intermediaries play in providing access to, managing, facilitating and mediating online speech. Rather than creating a platform for an influential few, as newspapers or broadcasters do, Internet intermediaries facilitate speech directly by individuals, giving everyone a platform and access to a global audience. By the same token, however, this grants these intermediaries an unprecedented influence over individuals' right to freedom of expression and access to information. This power has also attracted the attention of State actors, which are placing increasing pressure on online intermediaries to facilitate and/or participate in human rights violations, for example by supporting intrusive surveillance systems or acting to police user content.

In recent years, there has been an increasing focus on the human rights implications of the policies and practices of intermediaries. The most high profile work on human rights and the private sector in general is the 2011 *Guiding Principles on Business and Human Rights*,[5] which was developed under the auspices of the United Nations. However, recent years have seen the launch of programmes aimed specifically at the tech sector, such as the Global Network Initiative[6] and the Ranking Digital Rights Project.[7]

There are three layered challenges which any initiative to promote good practice in the private sector faces. The first is engagement in the sense of simply getting major

[3] Resolution A/HRC/20/L.13, 29 June 2012. Available at: www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc.
[4] Resolution A/C.3/68/L.45/Rev.1, 26 November 2013. Available at: www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1.
[5] UN OHCHR, Guiding Principles On Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, 16 June 2011, HR/PUB/11/04. Available at: www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.
[6] See: www.globalnetworkinitiative.org.
[7] Rebecca Mackinnon, "The Ranking Digital Rights 2015 Corporate Accountability Index is now online!", Ranking Digital Rights, 3 November 2015. Available at: rankingdigitalrights.org/.

private sector actors to the table. The second is transparency, in terms of being able to access corporate information in order to assess performance, and then of being able to publish the results of those assessments. The third is actually fostering change, and convincing companies to amend policies or practices which are problematic or which do not represent better practice.

These are significant challenges, which are in some respects more complicated than efforts to promote human rights at the State level (itself no easy task). Furthermore, solidarity from States in promoting respect by other States is common, whether conducted on a bilateral basis or through intergovernmental organisations, while the presence of strong competition tends to undermine such solidarity among private companies. Nonetheless, the growing importance of intermediaries in this area means that the human rights community must face these challenges, and work to promote greater respect for human rights by intermediaries. The major areas of engagement can be divided thematically into six key issues, as spelled out in the following sections.

Expanding Access

Expanding access to the Internet is key to promoting human rights on the Internet, so that the benefits conferred may be enjoyed as widely as possible. Over the past decades, significant access gaps have emerged, including between developed and developing countries, between urban and rural populations and, most importantly, between the better off and the poor.[8] These discrepancies are the result of various factors. For example, urban areas are smaller and have a higher population density, and are thus easier and cheaper to connect. Cost differentials may be passed on to consumers, even though urban dwellers tend to be wealthier than rural ones. Intermediaries, and particularly access providers, can play a role in helping to overcome these divides by taking action to mitigate or eliminate pricing differentials between rural and urban customers. Access providers should also work directly to expand access, by investing a reasonable proportion of their profits in creating new infrastructure, including potentially through entering into public-private partnerships to this end.

While costs and a lack of infrastructure are major challenges to expanding access, linguistic or social barriers also inhibit the Internet's spread. These challenges can be self-reinforcing, since the lack of a likeminded community online can lead to a dearth of relevant content, further reducing the interest of members of that group in connecting. Again, intermediaries have an important role to play in overcoming these barriers, for example by promoting the development of content of relevance to less connected communities or in smaller languages.

[8] Brahima Sanou, ICT Facts & Figures (May 2015: International Telecommunication Union (ITU) Telecommunication Development Bureau). Available at: www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

Beyond their responsibility to help expand access, it is important to consider the role intermediaries can play vis-à-vis State efforts to limit access, for example by cutting off or denying service to users. These measures are highly intrusive and almost never justified according to international standards regarding freedom of expression. Where a government demands that an access provider cut off or deny service to a user or group, the provider should consider the broader human rights implications and any viable alternatives. Providers should also resist these demands to the extent that this is reasonable and should, as far as this is legally permitted, be transparent about requests they receive to cut off access.

Net Neutrality

As the Internet has grown, and become more lucrative, the ongoing debate about the foundational principle of network neutrality has sharpened. The core idea behind this principle is that intermediaries should not favour or disfavour (discriminate against) the transmission of certain types of Internet traffic.[9] There are several reasons why net neutrality is fundamentally important, including that it promotes free competition and that it limits the ability of private intermediaries to control online speech and debates.

States have approached this issue in different ways. Although the Internet and the way it is used are constantly changing, and there is no single and immutable rule for how networks should be managed, certain fundamental principles should guide intermediaries in this area. First and foremost, policies and technical protocols for managing Internet traffic should aim to improve the functioning of the Internet for all users, rather than favouring traffic from or to users who pay a premium or who have preferential or partnership arrangements. Transparency is also important, including publishing information about policies and technical protocols for managing traffic and periodic reports providing summaries about how traffic and information was handled. Where net neutrality principles are codified in law, intermediaries should respect this and avoid lobbying for change. Where the law is unclear or unsettled, they should still act in ways that respect the core principles of network neutrality.

A particularly contentious aspect of the net neutrality debate concerns zero rating schemes, which provide cheap or free access to the Internet but only give access to a limited range of services. Free Basics, a Facebook-led initiative which essentially provides people with free access to a few Internet services, including Facebook, is among the most well known zero rating schemes. Its proponents claim that by offering users a stripped-down version of the Internet for free, Free Basics generates interest in the Internet among new potential users, who can then move on to pay for a full connection. However, Free Basics has also faced criticism for failing

[9] There are recognised exceptions to this rule, such as where necessary to protect the integrity or security of a network or to combat spam. For a more detailed description of these issues, see: www.thisisnetneutrality.org/.

to respect the principle of net neutrality and has even been banned by some regulatory agencies.[10] Although it can be argued that the harm inherent in zero rating schemes is outweighed by their benefit in bringing new people online, other schemes for providing an "on ramp" to the Internet do not compromise net neutrality. As a result, and due to the broad public interest in protecting net neutrality, the onus rests on intermediaries which have proposed or are operating zero rating schemes which compromise net neutrality to demonstrate that they are clearly more effective in terms of bringing people online than schemes which respect net neutrality and that the benefits are significant enough to justify these compromises.

Moderation and Removal of Content

Among the major factors behind the success of the Internet has been the open, honest and freewheeling nature of online discourse. By the same token, the sense of anonymity that is associated with being behind a computer or mobile screen can also encourage people's darker impulses and the Internet is a prime vehicle for vitriol and threats, as well as for the distribution of illegal material. This places intermediaries in a difficult position. On the one hand, for many the free flow of information is their bread and butter. On the other hand, their growing influence has placed them under increasing pressure, including from their own users, to mitigate the less desirable forms of online speech. Gender-based harassment is notoriously endemic online, although it is only part of a broader "civility" problem.

This has led some intermediaries to engage in more active content management which, in turn, has given rise to difficult challenges in determining when and how forcefully to intervene. It is conceptually easy to defend a laissez-faire approach, where companies only intervene when they are legally required to do so, on freedom of expression grounds. Once companies choose to go beyond that, the debate becomes far more tangled. In 2014, Twitter reacted energetically against the spread of propaganda messages about the murder of journalist James Foley at the hands of the Islamic State.[11] Although few would fault them for taking this stand, it inevitably led to questions as to why they had not been similarly proactive in working to combat sexual or racial harassment.[12] In 2012, a series of articles drew attention to forums on Reddit devoted to sexualising underage girls. Reddit

[10] The most energetic campaign against Free Basics has emerged in India under the banner "Save the Internet". A summary of arguments against the programme is available at: blog.savetheinternet.in/what-facebook-wont-tell-you-about-freebasics/.

[11] Shane Harris, "Social Media Companies Scramble to Block Terrorist Video of Journalist's Murder", Foreign Policy, 19 August 2014. Available at: foreignpolicy.com/2014/08/20/social-media-companies-scramble-to-block-terrorist-video-of-journalists-murder/.

[12] James Ball, "Twitter: from free speech champion to selective censor?" The Guardian, 21 August 2014. Available at: www.theguardian.com/technology/2014/aug/21/twitter-free-speech-champion-selective-censor?CMP=twt_gu.

ultimately decided to ban the content, a decision their users contrasted with the website's continued hosting of a forum devoted to pictures of dead children.[13]

Ultimately, private sector intermediaries have considerable flexibility in terms of the material they classify as offensive or against the standards of their services, but clear communication and strong procedural protections are essential. Content moderation should be based on clear, pre-determined policies which can be justified by reference to a standard based on objective criteria (such as providing a family friendly service) and which are described clearly in the policy. Ideally, intermediaries should consult with their users when determining such policies. In addition, intermediaries should post clear, thorough and easy to understand guides to their policies and practices, carefully scrutinising complaints and applying their policies consistently.

Beyond intermediaries' self-imposed standards, significant issues arise in the context of how they respond to illegal material. A major factor here is whether, and under what circumstances, intermediaries are themselves protected against liability for content in relation to which they provide services. Many legal systems condition immunity on intermediaries removing problematic content once they have been notified about it. Experience suggests that this approach is ripe for abuse, particularly in the case of copyright. Frivolous copyright removal requests are frequently used as a tool to quash political dissent or remove information that a person or organisation finds embarrassing or inconvenient. Automated systems to flag copyrighted material have been found to make mistakes and they are generally unable to take into account possible defences to copyright infringement, such as fair practice (known as fair use or fair dealing in some jurisdictions).

Intermediaries obviously wish to shield themselves against legal liability. However, many also go significantly beyond minimum legal requirements. In order to combat misuse, it is important to build strong procedural protections into systems for addressing illegal content. Users whose content is subject to removal should, whenever this is legally permissible, be notified promptly and provided with information about the process and any opportunities to mount a defence. Intermediaries should also try to devise solutions which are minimally intrusive and as targeted as possible. Where an intermediary determines that content should be removed, they should retain the means to reverse that action for as long as any appeal against the decision is pending, and should offer users the option to preserve and export their data, unless it is patently illegal.

Addressing Privacy Concerns Online

[13] "Why is it that r/jailbait was shut down, but not r/picsofdeadkids?", Reddit, 7 September 2012. Available at: www.reddit.com/r/AskReddit/comments/zhd5d/why_is_it_that_rjailbait_was_shut_down_but_not/.

The right to privacy is recognised internationally as a human right, guaranteed in the *International Covenant on Civil and Political Rights*[14] and in most national constitutions. Privacy is also closely correlated with freedom of expression. Studies have shown that perceptions of control over one's communications, including over who has access to them, lead to franker and more extensive communications, while a loss of control leaves people feeling less free to engage earnestly.[15]

The Internet has had a dramatic impact on our understandings of the very concept of privacy. On the one hand, the Internet provides for an unprecedented level of freedom and anonymity. For a gay Ugandan or Russian, or a Saudi atheist, the Internet may provide the only avenue for self-expression or to network with likeminded communities. On the other hand, the Internet is also the most heavily monitored and tracked medium of expression in history, where every move that users make is noted, followed and recorded.

The collection and sale of personal information represents a core business model for many intermediaries. There are benefits to this, primarily in the form of allowing users to access services free of direct charges. But, even if one embraces the idea of exchanging privacy for free services online, States have a responsibility to protect consumers in these relationships.[16] It is arguable that the intrusiveness of State regulation over companies in this area should depend, at least in part, on the extent to which industry acts to offer effective protections of its own.

A key issue here is being clear and transparent with users about policies regarding the collection, sharing and processing of information. For example, users may implicitly understand that their private information is being processed by companies whose business model is based on advertising, but may not expect the same treatment from companies which impose up-front charges for their services.[17] Similarly, users may think that information will be tracked only in an automated or aggregated way, and assume that it will not be examined by human beings.[18] There is a particular need for clarity around the involvement of third party data brokers,

---

[14] UN General Assembly Resolution 2200A(XXI), 16 December 1966, in force 23 March 1976.
[15] Tamara Dinev, Heng Xu, Jeff H. Smith and Paul Hart, "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts" 22 European Journal of Information Systems (2013), p. 300. Available at: www.palgrave-journals.com/ejis/journal/v22/n3/pdf/ejis201223a.pdf.
[16] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, para. 58. Available at: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. See also Human Rights Committee, General Comment 16, 8 April 1988. Available at: tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en.
[17] Andy Greenberg, "How to Stop Apple From Snooping on Your OS X Yosemite Searches", Wired, 20 October 2014. Available at: www.wired.com/2014/10/how-to-fix-os-x-yosemite-search/.
[18] Andrew Crocker, "Microsoft Says: Come Back with a Warrant, Unless You're Microsoft", Electronic Frontier Foundation, 21 March 2014. Available at: www.eff.org/deeplinks/2014/03/microsoft-says-come-back-warrant-unless-youre-microsoft.

who generally have no direct relationship with the users and who often collate information from multiple sources, which can significantly compound the privacy interference.[19]

Although all companies have a duty to respect user privacy, those which explicitly market the privacy features of their services have a particular obligation to avoid privacy intrusive behaviour.[20] Intermediaries should not let their commercial interests undermine their obligation to make realistic representations to users about privacy and to respect these commitments.

Anonymous communication is a particularly important area of debate regarding online privacy. At a cultural level, many online communities have strong taboos against doxxing or publishing personally identifiable information about a person using an online alias.[21] Anonymity is particularly important in terms of facilitating communication about sensitive subjects, such as sexual or mental health issues or child abuse, and enabling whistleblowing. Websites like Wikileaks could not exist without the promises of anonymity which they provide. The central role the Internet plays in disseminating sensitive communications means that failures on this front can have especially severe consequences.

This is not to suggest that all intermediaries have a responsibility to allow people to use their services anonymously. Some intermediaries have legitimate reasons for requiring real-name registration. However, decisions about this should take into account the broader human rights implications and the impact that the requirement may have on users. In particular, intermediaries should not require real-name registration where it would significantly harm the rights of their users. Perceptions, and building realistic expectations, are of cardinal importance here, and intermediaries have a responsibility to be transparent with their users as to the extent to which any anonymity they offer or appear to be offering will be respected.

Another key user privacy issue is data security, including the use of encryption.[22] An increasing number of intermediaries are encrypting more user information by default.[23] This is a welcome shift, and intermediaries should also consider taking action to encourage stronger security practices among their users, for example by offering inducements for good practice. Beyond storing information in encrypted

[19] Timothy Libert, "Exposing the Hidden Web: Third-Party HTTP Requests on One Million Websites, International Journal of Communication, October 2015. Available at: ijoc.org/index.php/ijoc/article/download/3646/1503.
[20] See, for example, Paul Lewis and Dominic Rushe, "Revealed: how Whisper app tracks 'anonymous' users", The Guardian, 16 October 2014. Available at: www.theguardian.com/world/2014/oct/16/-sp-revealed-whisper-app-tracking-users.
[21] See: "What doxxing is, and why it matters", The Economist, 10 March 2014. Available at: www.economist.com/blogs/economist-explains/2014/03/economist-explains-9.
[22] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 22 May 2015, para. 56-63.
[23] Lorenzo Franceschi-Bicchierai, "Reddit Switches to Encryption By Default", Motherboard, 17 June 2015. Available at: motherboard.vice.com/read/reddit-switches-to-https-encryption-by-default.

formats whenever this is operationally and legally possible and supporting end-to-end encryption for users, data minimisation is another important factor in limiting privacy risks.[24] Once security has been breached, it is essential that intermediaries inform those who might have been impacted promptly and fully, since speed can be of the essence in mitigating the harm.

A final privacy issue is the right to be forgotten. In 2014, the European Court of Justice (ECJ) held that EU citizens had a right to request that search engines not display results relating to them which were "inadequate, irrelevant, or no longer relevant, or excessive in relation to the purposes for which they were processed".[25] There are legitimate concerns regarding how the Internet preserves and presents information about peoples' pasts. At the same time, there are significant problems with this judgment, particularly its failure to consider sufficiently the freedom of expression interests at play.

The decision is also problematic insofar as it places responsibility for implementation on search engines. Decisions about removing content should ideally be made by expert, public decision-makers, not private search engines. However, having been given this responsibility, search engines should implement it as fairly and transparently as possible. This should include consulting with key stakeholders to develop detailed policies and standards regarding how they enforce the right to be forgotten. Search engines should also, as far as possible, respect due process rights when applying the right to be forgotten, including by informing those whose content is subject to a removal request, as far as this is legally permitted, and by giving them an opportunity to argue that the material should not be blocked, including because the public interest lies in continuing to display the content.

Transparency and Informed Consent

The Internet has fundamentally changed our relationship with information, which has led to demand for greater openness on the part of intermediaries. This is particularly true in terms of users' personal information, where there is a broadly recognised right to track how it is being stored and processed.[26] The publication of certain types of information is also vital to facilitate informed consumer choices, including to allow people to choose companies whose policies align with their priorities and values.

---

[24] Federal Trade Commission, *Internet of things: Privacy and Security in a Connected World*, January 2015. Available at: www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[25] Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:2014:317. Available at: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

[26] Human Rights Committee, General Comment 16, 8 April 1988. Available at: tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en.

An important openness tool is transparency reporting, which has become relatively common among major tech firms. Although the specific information provided varies, the central aims are generally to profile requests to take down content and government attempts to access user information. Better practice is to provide as much detail as possible here, including by subdividing statistics according to the underlying basis for the request, the type and location of the requester, the date of the request, how the user who was the subject of the complaint was notified and after what period of time, and how the request was disposed of. Information about the nature and processing of requests by governments for user information should be made available as far as such disclosures are legally permitted. Intermediaries should also publish information about their own enforcement of their terms of service, including where content is automatically flagged by a particular algorithm or where users have their accounts deleted for committing some sort of prohibited action.

Ideally, transparency reporting should be standardised across particular categories of intermediaries, although there are significant practical and legal complications to achieving this. At present, the differences in reporting make it difficult to compare policies and practices among actors operating in the same industry sector.

Beyond transparency reporting, published terms of service are an important vehicle for openness. Unfortunately, users seldom engage with these documents, despite the fact that they serve as the legal basis for the relationship between the company and its users. In many cases, this includes the core agreement whereby users trade their privacy for services, an exchange which is predicated on informed consent. The fact that users so rarely pay attention to the content of terms of service also gives companies a licence to draft these terms broadly and/or in a deliberately obscure manner. For many companies, it is difficult even for a careful reader to deduce the practical implications of their terms of service. This inaccessibility, in turn, discourages users from reading the terms at all.

The potential breadth of Facebook's Data Policy, for example, was laid bare in October 2014, when the company published a paper revealing that it had been "experimenting" on how slight changes to the site could impact on users' political engagement or mood.[27] The idea of a formal experiment on 61 million unsuspecting subjects raised concerns, particularly in light of the potential for large-scale social manipulation. The company defended the experiment in part by noting references to academic research in their Data Policy. Nonetheless, it is likely that, if users who signed up for a Facebook account were presented with a clear, bold message saying that the company intended to use them to carry out social and behavioural experiments, at least a few may have reconsidered.

[27] Micah L. Sifry, "Facebook Wants You to Vote on Tuesday. Here's How It Messed With Your Feed in 2012", Mother Jones, 31 October 2014. Available at: www.motherjones.com/politics/2014/10/can-voting-facebook-button-improve-voter-turnout.

This is not to minimise the legitimate challenges that intermediaries face in engaging users on these issues, and the difficulty of reducing a document that has legal implications to simple, user-friendly terms. Nonetheless, more needs to be done to ensure that terms of service and other polices are clear. The increasing publication of "simplified" terms is a good start, though these must be crafted carefully to avoid painting an inaccurate picture. Recent years have also seen independent initiatives aimed at enhancing user understanding of intermediaries' policies, which intermediaries should support.[28]

Consultation is also important and intermediaries should consult with users prior to making major amendments to their terms of service, notify users of any amendments they do make and make previous versions available so that users can understand the changes. Ideally, outreach should go even further, including by providing avenues of engagement for users seeking clarification of their terms of service or other policy questions, and by allowing users to propose policy changes.

Responding to State Attacks on Freedom of Expression

Many intermediaries face the challenge of what to do when confronted by government demands which do not accord with international human rights standards. The responsibility to avoid complicity in human rights violations is a key part of the UN's Protect, Respect and Remedy framework,[29] as well as the main focus of the GNI.

Some of the most challenging cases of private sector complicity in human rights violations involve China, which has not only demanded compliance with invasive censorship demands but also sought to enlist private sector collaboration in persecuting prominent critics, and even in supporting State cyber attacks.[30] The country has been particularly bold in taking action against companies that refuse to acquiesce to their demands, including by blocking them from the lucrative Chinese market. Although China is the most high profile and extreme example, companies face similar dilemmas in other countries, including sometimes in developed democracies.

No government, of course, has a perfect human rights record. What constitutes a legitimate restriction on freedom of expression is a complex question and different countries have different rules. By and large, it is reasonable to expect intermediaries to comply with local laws on these issues in the jurisdictions where they operate.

---

[28] An example of this is "Terms of Service; Didn't Read". Available at: tosdr.org/.
[29] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, 7 April 2008. Available at: www.reports-and-materials.org/sites/default/files/reports-and-materials/Ruggie-report-7-Apr-2008.pdf.
[30] Bill Marczak and Nicholas Weaver, "China's Great Cannon", Munk School of Global Affairs, 10 April 2015. Available at: citizenlab.org/2015/04/chinas-great-cannon/.

But more active steps to avoid complicity in human rights abuses are warranted when operating in countries with poor human rights records.

Intermediaries should carefully assess the risks whenever a new potentially risky market is entered or a new product is launched, and develop strategies to mitigate these, for example by disabling features which may be prone to misuse in a particular national context or by avoiding locating their employees or storing data in countries which have a poor record of respecting human rights. Most global tech companies only maintain a physical presence in a few countries, and other States have no real legal means to compel compliance with their demands, other than by threatening to deny the company access to their market. Being shut out of a country is obviously not a consequence to be taken lightly, given the commercial implications. However, if the major players put up a unified front in support of human rights, it will be difficult for countries to ban them all (although China may represent an exception here).

Intermediaries will need to consider carefully whether a violation is significant enough to warrant noncompliance with domestic law. Although the line can be difficult to draw, where an intermediary encounters a case of their systems or services being subverted to support a clear and grave violation of human rights, they have a responsibility to take action to avoid or mitigate complicity. This can include refusing to turn over records that support a political prosecution or to participate in widespread systems of repression, such as China's Great Firewall. Relevant considerations here include the number of users impacted, the severity of the interference and the broader human rights context in which the interference takes place, including the country's overall human rights record.

Where a State-mandated interference falls short of a clear and grave violation of human rights, intermediaries should only hand over information when subject to a legal requirement to do so and should notify users who are subject to a government request as soon as this is legally allowed. Where realistic legal avenues for contesting problematic laws or policies exist, intermediaries have some responsibility to launch legal challenges in appropriate cases and to stand up for the rights of their users. Intermediaries should also explore their options for seeking external leverage, such as soliciting diplomatic support from supportive governments or from intergovernmental organisations, and to liaise with one another to establish a unified front.